REMARKS/ARGUMENTS

Claims 1-21 are pending. Claims 1, 5, and 10-12 are amended herein. No new matter is added as a result of the Claim amendments.

35 U.S.C. § 102 Rejections

Claims 1, 2, 4-6, and 8-13, and 15-21 are rejected under 35 U.S.C. § 102 (a) as being anticipated by Hardy et al. (U.S. Pub. No. 20020152392), hereinafter referred to as "Hardy." The Applicants respectfully submit that the claim limitations recited in Claims 1, 2, 4-6, and 8-13, and 15-21 of the present invention are neither taught nor suggested by Heath. For example, Claim 1 of the present invention recites (emphasis added):

> A method of windowed backward key generation, comprising:
> a) providing information to a user that allows <u>determining a limited number of previous keys in a series of keys</u> from a later key in the series <u>and wherein said information is derived from at least one of said limited number of previous key in said series</u>;
> b) generating a key in the series, based at least in part on said information provided to said user;
> c) providing said key in the series to the user; and
> d) <u>said user determining at least one key in the limited number of previous keys in the series by applying said information to said key in the series provided to the user.</u>

Claim 8 of the present invention recites (emphasis added):

> A method of windowed backward key rotation, comprising:
> a) providing to a user a key rotation element and a key (K_i), wherein later versions of the key rotation element are determinable by the user but previous versions of the key rotation element are not determinable by said user;
> b) generating a later version of the key (K_{i+n}) based on a later version of the key rotation element, wherein "n" is a positive integer;
> c) providing to the user the later version of the key (K_{i+n}); and
> d) <u>said user determining a version of the key from (K_i-K_{i+n+1}), inclusive, by applying a version of the key rotation element to a version of the key from (K_{i+1}-K_{i+n}), inclusive.</u>

Claim 15 of the present invention recites (emphasis added):

> A method of windowed backward file key generation, comprising:
> a) generating an initial file key;
> b) generating an initial key rotation exponent, wherein <u>said initial key rotation exponent allows previous versions of file keys to be determined back until a pre-determined version of the file key</u>, but no file keys further back; and
> c) providing said initial file key and said initial key rotation exponent to initial users.

With reference to Claim 1, the Applicants respectfully submit that Hardy does not teach or suggest providing information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series and which is derived from at least one of said limited number of previous key in said series. Instead, the Applicants understand the teaching of Hardy to suggest that for each previous, or subsequent, version of a software product being accessed by a user, a unique key is generated which is independent of any other keys used to decrypt the software product. Because the new key is not derived from any previous key in a series of keys, the Applicants respectfully submit that the keys generated in the teaching of Hardy cannot be used to determine any previous key in a series of keys as recited in Claim 1. Thus, the Applicants respectfully submit that Hardy teaches away from the claim limitations recited in Claim 1.

More specifically, the Applicants understand the teaching of Hardy to suggest that a unique key is generated for each prior or subsequent software update that a user wants to access and that this key is independent of any previous or subsequent keys. In paragraph [0021], Hardy describes a process 40 for generating a new key in which he states (emphasis added);

"As indicated by step 42, the manufacturer first generates new encryption KEY B. KEY B can be generated by a random number generator for instance. The Different Version of the Software Product 39 is then encrypted with KEY B as indicated by step 43 sometime before release delivery."

Thus, the Applicants respectfully submit that KEY B is a new decryption key which is not related or derived from a series of previous keys in a series and is therefore of no use in determining any previous key in a series of keys. Additionally, in citing the use of a random number generator, Hardy teaches away from the limitations recited in Claim 1 of the present invention of providing information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series and which is derived from at least one of said limited number of previous key in said series. Furthermore, there is no indication that the KEY B described by Hardy can be used to determine a limited number of previous keys in a series of keys as recited in Claim 1 of the present invention. Instead, the Applicants understand the teaching of Hardy to indicate that each new key generated by the random number generator is not related to a key used with previous, or subsequent, software version and is only

applicable to the particular version of the software product being accessed by the user. Hardy also teaches away from the limitations recited in Claim 1 in paragraph [0007] in which he states (emphasis added)," Moreover, it is desired that either sequential or non-sequential keys be independent of previous keys." Thus, the Applicants respectfully submit that the rejections of Claim 1 under 35 U.S.C. § 102 (a) are also not supported by the cited reference.

Claims 9-14 depend from Claim 8 and recite additional limitations descriptive of embodiments of the present invention. Accordingly, the Applicants respectfully submit that the rejection of Claims 9-14 under 35 U.S.C. § 102 (a) are also not supported by the cited reference.

With reference to Claim 8, the Applicants respectfully submit that Hardy does not teach or suggest the claim limitations recited in Claim 8. More specifically, the Applicants submit that the method of Hardy is incapable of determining a version of a key from $(K_i - K_{i+n+1})$, inclusive, by applying a version of a key rotation element to a version of a key from $(K_{i+1} - K_{i+n})$, inclusive. Instead, the method of Hardy generates a key which is independent of any previous, or subsequent, keys used to access a software application. Because each key is independently generated, a key rotation element would be useless in determining a version of a key from $K_i - K_{i+n+1}$ inclusive as recited in Claim 8 of the present invention. Thus, the Applicants respectfully submit that the rejections of Claim 8 under 35 U.S.C. § 102 (a) are also not supported by the cited reference.

Claims 2-7 depend from Claim 1 and recite additional limitations descriptive of embodiments of the present invention. Accordingly, the Applicants respectfully submit that the rejection of Claims 2-7 under 35 U.S.C. § 102 (a) are also not supported by the cited reference.

With reference to Claim 15, the Applicants respectfully submit that the method of Hardy is incapable of generating an initial key rotation exponent which allows previous versions of file keys to be determined back until a pre-determined version of the file key, but no file keys further back. Instead, the file keys generated by Hardy are independent of any other file keys, due to the use of a random number

generator, and cannot be used to determine a previous version of a file key, much less a plurality of file keys of a series as recited in Claim 15 of the present invention. Thus, the Applicants respectfully submit that the rejections of Claim 15 under 35 U.S.C. § 102 (a) are also not supported by the cited reference.

Claims 16-21 depend from Claim 15 and recite additional limitations descriptive of embodiments of the present invention. Accordingly, the Applicants respectfully submit that the rejection of Claims 16-21 under 35 U.S.C. § 102 (a) are also not supported by the cited reference.

35 U.S.C. § 103 Rejections

Claims 3, 7, and 14 are rejected under 35 U.S.C. § 103 (a) as being unpatentable over Hardy. With reference to Claim 3, the Applicants respectfully submit that Hardy, does not teach or suggest providing to the user a key rotation exponent which is derived from at least one of a limited number of previous keys in a series and is used to determine a previous key in the series from a later key in the series by exponentiating said later key by the key rotation exponent as discussed above with reference to Claim 1. As discussed above with reference to Claim 1, the Applicants submit that the method of Hardy is incapable of determining a previous key in a series of keys as recited in Claim 1. More specifically, because each key is independently generated by a random number generator, the method of Hardy cannot be expected to determine a previous key in a series from a later key in the series. Thus, the Applicants respectfully submit that the rejection of Claim 3 under 35 U.S.C. § 103(a) is not supported by the cited reference.

With reference to Claims 7 and 14, the Applicants respectfully submit that the method of Hardy is incapable of operating in the manner recited in either of Claims 1 and 8 of the present invention. Accordingly, the Applicants respectfully submit that the rejection of Claim 7, which depends from Claim 1, under 35 U.S.C. § 103(a) is not supported by the cited reference.

Similarly, the Applicants respectfully submit that the rejection of Claim 14 which depends from Claim 8, under 35 U.S.C. § 103(a) is not supported by the cited reference.

CONCLUSION

In light of the above remarks, the Applicants respectfully request reconsideration of the rejected Claims.

Based on the arguments presented above, the Applicants respectfully assert that Claims 1-21 overcome the rejections of record and, therefore, the Applicants respectfully solicit allowance of these Claims.

The Applicants have reviewed the references cited but not relied upon. The Applicants did not find these references to show or suggest the present Claimed invention: U.S. Patent No. 6,363,149.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 7/3/07

John P. Wagner, Jr.
Reg. No. 35,398
123 Westridge Drive
Watsonville, CA 95076 USA
(408) 316-1767